Maximum number of common zeros of homogeneous polynomials over finite fields

Beelen, Peter ; Datta, Mrinmoy; Ghorpade, Sudhir Ramakant

Published in:
Proceedings of the American Mathematical Society

Link to article, DOI:
10.1090/proc/13863

Publication date:
2017

Document Version
Peer reviewed version

Maximum Number of Common Zeros of Homogeneous Polynomials over Finite Fields

Peter Beelen, Mrinmoy Datta, Sudhir R. Ghorpage

Abstract

About two decades ago, Tsfasman and Boguslavsky conjectured a formula for the maximum number of common zeros that r linearly independent homogeneous polynomials of degree d in $m+1$ variables with coefficients in a finite field with q elements can have in the corresponding m-dimensional projective space. Recently, it has been shown by Datta and Ghorpade that this conjecture is valid if r is at most $m+1$ and can be invalid otherwise. Moreover a new conjecture was proposed for many values of r beyond $m+1$. In this paper, we prove that this new conjecture holds true for several values of r. In particular, this settles the new conjecture completely when $d=3$. Our result also includes the positive result of Datta and Ghorpade as a special case. Further, we determine the maximum number of zeros in certain cases not covered by the earlier conjectures and results, namely, the case of $d=q-1$ and of $d=q$. All these results are directly applicable to the determination of the maximum number of points on sections of Veronese varieties by linear subvarieties of a fixed dimension, and also the determination of generalized Hamming weights of projective Reed-Muller codes.

1 Introduction

Let d, m be positive integers and let $\mathbb{F}_q$ denote the finite field with q elements. Let us denote by S the ring $\mathbb{F}_q[X_0, X_1, \ldots, X_m]$ of polynomials in $m+1$ variables with coefficients in $\mathbb{F}_q$ and by S_d its dth graded component, i.e., let S_d be the space of all homogeneous polynomials in S of degree d (including the zero polynomial). Given any homogeneous polynomials $F_1, \ldots, F_r \in S$, let $\mathsf{V}(F_1, \ldots, F_r)$ denote the corresponding projective algebraic variety over $\mathbb{F}_q$, i.e., the set of all $\mathbb{F}_q$-rational common zeros of $F_1, \ldots, F_r$ in the m-dimensional projective space $\mathbb{P}^m$. Now fix a positive integer $r \leq \dim_{\mathbb{F}_q} S_d = \binom{m+d}{d}$. We are primarily interested in determining

$$e_r(d,m) := \max\left\{|\mathsf{V}(F_1,\ldots,F_r)| : F_1,\ldots,F_r \in S_d \text{ linearly independent}\right\}. \tag{1}$$

The first nontrivial case is $r=1$ and here it was conjectured by Tsfasman in the late 1980's that

$$e_1(d,m) = dq^{m-1} + p_{m-2} \quad \text{whenever } d \leq q, \tag{2}$$

where for any integer k,

$$p_k := \begin{cases} |\mathbb{P}^k(\mathbb{F}_q)| = q^k + q^{k-1} + \cdots + q + 1 & \text{if } k \geq 0, \\ 0 & \text{if } k < 0. \end{cases}$$

The conjecture was proved in the affirmative by Serre [9] and, independently, by Sørensen [10] in 1991. Later in 1997, Boguslavsky [1] showed that

$$e_2(d,m) = (d-1)q^{m-1} + q^{m-2} + p_{m-2} \quad \text{whenever } 1 < d < q-1.$$

In the same paper, Boguslavsky [1] made several conjectures, ascribing some of them to Tsfasman. Surmising from the conjectural statements and results in [1], one arrives at the Tsfasman-Boguslavsky Conjecture (TBC), which states that

$$e_r(d,m) := p_{m-2j} + \sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) \quad \text{whenever } 1 \le d < q-1,$$

where $(\nu_1, \ldots, \nu_{m+1})$ is the rth element in descending lexicographic order among $(m+1)$-tuples $(\alpha_1, \ldots, \alpha_{m+1})$ of nonnegative integers satisfying $\alpha_1 + \cdots + \alpha_{m+1} = d$, and $j := \min\{i : \nu_i \neq 0\}$.

The conjectural formula above for $e_r(d.m)$ was motivated by the computations of Boguslavsky [1, Lem. 4] for the number of $\mathbb{F}_q$-rational points of the so-called linear (r, m, d)-configurations, and a conjecture of Tsfasman [1, Conj. 1]. For details about these, see [1, § 2] and [3, Rem. 3.6]. The TBC remained open for a considerably long time. However, two important developments took place shortly after Boguslavsky's paper was published. First, working on a seemingly unrelated question (and unaware of the TBC), Zanella [11] determined $e_r(2, m)$ completely. Second, Heijnen and Pellikaan [6], found exact formulae for the affine analogue of (1), namely,

$$e_r^{\mathbb{A}}(d,m) := \max\left\{ |\mathsf{Z}(f_1, \ldots, f_r)| : f_1, \ldots, f_r \in T_{\le d} \text{ linearly independent} \right\},$$

where T denotes the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_m]$ in m variables over $\mathbb{F}_q$ and $T_{\le d}$ the set of polynomials in T of degree $\le d$, and for any $f_1, \ldots, f_r \in T$, $\mathsf{Z}(f_1, \ldots, f_r)$ denotes the set of all $\mathbb{F}_q$-rational common zeros of $f_1, \ldots, f_r$ in the m-dimensional affine space $\mathbb{A}^m$. The result of Heijnen-Pellikaan can be stated as follows.

$$e_r^{\mathbb{A}}(d,m) = H_r(d,m) := \sum_{i=1}^{m} \beta_i q^{m-i} \quad \text{whenever } 1 \le d < q,\ m \ge 1, \text{ and } 1 \le r \le \binom{m+d}{d}, \quad (3)$$

where $(\beta_1, \ldots, \beta_m)$ is the rth element in descending lexicographic order among all m-tuples $(\gamma_1, \ldots, \gamma_m)$ of nonnegative integers satisfying $\gamma_1 + \cdots + \gamma_m \le d$.

Recently, it was shown in [3] that the TBC is false, in general, by showing that $e_r(d, m)$ can be strictly smaller than the conjectured quantity if $r > m + 1$. Further, in [4] it was shown that the TBC holds in the affirmative if $r \le m + 1$; this gives

$$e_r(d,m) = (d-1)q^{m-1} + \lfloor q^{m-r} \rfloor + p_{m-2} \quad \text{if } 1 < d < q-1 \text{ and } r \le m+1. \quad (4)$$

While this settles in a way the Tsfasman-Boguslavsky Conjecture, there still remains the question of determining $e_r(d, m)$ in all the remaining cases. In fact, besides (2), (4), and the result of Zanella for $e_r(2, m)$ mentioned earlier (see Theorem 2.10), the only other known results about $e_r(d, m)$ are the following. First, it is easy to determine $e_r(d, m)$ for the initial values of d or m for all permissible r, that is, for $1 \le r \le \binom{m+d}{d}$. More precisely, we have

$$e_r(1,m) = p_{m-r} \text{ for } 1 \le r \le m+1. \quad \text{and} \quad e_r(d,1) = d-r+1 \quad \text{for } 1 \le r \le d+1 \text{ and } d \le q; \quad (5)$$

see, for instance, [4, § 2.1]. It is not difficult to determine $e_r(d, m)$ for some terminal values of r:

$$e_r(d,m) = \tbinom{m+d}{d} - r \quad \text{for } \tbinom{m+d}{d} - d \le r \le \tbinom{m+d}{d} \text{ and } d < q-1. \quad (6)$$

A proof can be found in [5, Thm. 4.7]. At any rate, the results obtained thus far do not yield the exact values of

- $e_r(d, m)$ whenever $m + 1 < r < \binom{m+d}{d} - d$ and $2 < d < q - 1$

- $e_r(d,m)$ whenever $1 < r \leq \binom{m+d}{d}$ and $d \geq q-1$

Note also that the case $d \geq q+1$ is trivial for many values of r (see [4, Rem. 6.2] for more details). But the cases $d = q-1$ and $d = q$ were unresolved for most values or r and m, and it is conceivable that the TBC may even be valid in some of them, at least when $r \leq m+1$. For going beyond $r = m+1$, a conjecture that ameliorates the TBC was made in [4] for many (but not all) values of r and for values of d up to and including $q-1$. The conjecture simply states that

$$e_r(d,m) = H_r(d-1,m) + p_{m-1} \quad \text{if } 1 < d \leq q-1 \text{ and } r \leq \binom{m+d-1}{d-1}. \tag{7}$$

where $H_r(d-1,m)$ is as in (3) except with d replaced by $d-1$.

We can now describe the contents of this paper. Our main result (Theorem 5.3) is an affirmative solution of the new conjecture (7) when $d > 2$ and $r \leq \binom{m+2}{2}$. In particular, this completely proves the conjectural formula (7) when $d = 3$. Furthermore, while our methods are partly inspired by those in [4], the results of [4] are not used directly. As such our results yield (4) as a corollary. In fact, we do a little better, since the case $d = q-1$ is also covered, and moreover, the proof is somewhat simpler. Our second main result (Theorems 6.2 and 6.3) is the determination of $e_r(d,m)$ in the case $d = q$ and $1 \leq r \leq m+1$. The result matches with the answer predicted by the TBC as well as (4) and (7) when $r = 1$ and $r = m+1$, but not otherwise.

The key ingredients in our proofs are as follows. We make use of the nontrivial results of Heijnen and Pellikaan [6] as well as Zanella [11]. In addition, we utilize an inequality of Serre/Sørensen [9, 10], a variant of Bézout's theorem by Lachaud and Rolland [8], a simple lemma given by Zanella [11] (see also [3, Rem. 2.3]), and an inequality of Homma and Kim [7] about the maximum number of points on a hypersurface without an $\mathbb{F}_q$-linear component. Another important ingredient in our proof is the use of a quantity that we call the t-invariant associated to a linear space of homogeneous polynomials of the same degree. This notion can be traced back to the proof of [5, Thm. 5.1] in a special case, but here it is used more systematically.

We remark here that the determination of $e_r(d,m)$ is equivalent to the determination of the maximum number of $\mathbb{F}_q$-rational points on linear sections $\mathscr{V}_{m,d} \cap L$ of the Veronese variety $\mathscr{V}_{m,d}$ corresponding to the d-uple embedding of $\mathbb{P}^m$ in $\mathbb{P}^{M-1}$, where $M = \binom{m+d}{d}$ and where L varies over linear subvarieties of $\mathbb{P}^{M-1}$ of codimension r. Moreover, finding $e_r(d,m)$ is essentially the same as finding the rth generalized Hamming weight of the projective Reed-Muller code $\mathrm{PRM}_q(d,m)$ of order d and length p_m. Also, results on the determination of $e_r(d,m)$ complement the recent result of Couvreur [2] on the number of points of projective varieties of given dimensions and degrees of its irreducible components. These connections are explained in [3, 5], and one may refer to them for more details on these aspects.

2 Preliminaries

Fix for the remainder of this paper a prime power q and positive integers d, m, r. In subsequent sections and subsections, some further assumptions on d or m or r will be made, depending on the context. For the convenience of the reader, the basic underlying assumptions, if any, will be specified in the "context" mentioned at the beginning of the section or subsection. We will denote by $\mathbb{N}$ the set of all nonnegative integers and by $\mathbb{N}^m$ the set of m-tuples of nonnegative integers. We will continue to use the notations introduced in the previous section. In particular, given any subset W of $S := \mathbb{F}_q[X_0, X_1, \ldots, X_m]$, we denote by $\mathsf{V}(W)$ the set of $\mathbb{F}_q$-rational points of the corresponding projective variety in $\mathbb{P}^m$, i.e., $\mathsf{V}(W) := \{P \in \mathbb{P}^m(\mathbb{F}_q) : F(P) = 0 \text{ for all } F \in W\}$. If $W = \{F_1, \ldots, F_r\}$ or if W is a $\mathbb{F}_q$-linear subspace of S spanned by $F_1, \ldots, F_r$, then we may write $\mathsf{V}(F_1, \ldots, F_r)$ for $\mathsf{V}(W)$. Likewise, given any subset U of $T := \mathbb{F}_q[X_1, \ldots, X_m]$, we shall

denote by $\mathsf{Z}(U)$ the set $\{P \in \mathbb{A}^m(\mathbb{F}_q) : f(P) = 0 \text{ for all } f \in U\}$. If $U = \{f_1, \ldots, f_r\}$ or if U is a subspace of T spanned by $f_1, \ldots, f_r$, then we may write $\mathsf{Z}(f_1, \ldots, f_r)$ for $\mathsf{Z}(U)$. Note that we use the word *algebraic variety* as synonymous with *algebraic set*, i.e., a variety need not be irreducible. When we speak of geometric attributes such as dimension or degree of an (affine or projective) algebraic variety such as $\mathsf{V}(W)$ or $\mathsf{Z}(U)$, it will always be understood that it is the same as the dimension or degree of the corresponding variety over an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.

2.1 Projective Hypersurfaces and Affine Varieties

We recall here several results from the literature that we will need later on. Let us begin with the result of Serre [9] and Sørensen [10] (see also [3]) that was mentioned in the Introduction.

Theorem 2.1. *Let F be any nonzero homogeneous polynomial in S of degree d. Then*

$$|\mathsf{V}(F)| \leq dq^{m-1} + p_{m-2}.$$

Moreover $e_1(d, m) = dq^{m-1} + p_{m-2}$ whenever $d \leq q$.

Next, we recall a variant of Bézout's Theorem given by Lachaud and Rolland [8, Cor 2.2]. It should be noted that since S as well as T are unique factorization domains, a gcd (= greatest common divisor) of any finite collection $F_1, \ldots, F_r$ of polynomials in either of these rings exists and is unique up to multiplication by a nonzero scalar, and it may be denoted by $\gcd(F_1, \ldots, F_r)$. Note also that in case $F_1, \ldots, F_r$ are homogeneous, then so is their gcd.

Theorem 2.2. *Let $f_1, \ldots, f_r \in T$ be nonzero polynomials such that $\mathsf{Z}(f_1, \ldots, f_r)$ is an affine algebraic variety of dimension s. Then*

$$|\mathsf{Z}(f_1, \ldots, f_r)| \leq \deg(f_1) \cdots \deg(f_r) q^s.$$

In particular we have

$$|\mathsf{Z}(f_1)| \leq \deg(f_1) q^{m-1}$$

and

$$|\mathsf{Z}(f_1, f_2)| \leq \deg(f_1) \deg(f_2) q^{m-2}, \quad \textit{provided} \quad \gcd(f_1, f_2) = 1.$$

Proof. The first assertion is [8, Cor 2.2]. The next two are immediate consequences because if $f_1 \in T$ is nonconstant, then the hypersurface $\mathsf{Z}(f_1)$ has codimension 1 in $\mathbb{A}^m$, whereas if $f_1, f_2 \in T$ are coprime of positive degrees, then arguing as in the proof of [4, Lem. 2.2], we see that the codimension of $\mathsf{Z}(f_1, f_2)$ is 2. The case when $\deg(f_i) = 0$ for some $i = 1, 2$, is trivial. □

Let us deduce a refinement of the last result, which will be useful to us later.

Lemma 2.3. *Assume that $r \geq 2$. Let $f_1, \ldots, f_r \in T_{\leq d}$ be linearly independent polynomials such that $\gcd(f_1, \ldots, f_r) = 1$. If $\deg(f_1) \leq d - 1$, then*

$$|\mathsf{Z}(f_1, \ldots, f_r)| \leq (d-1) dq^{m-2}.$$

If, in addition, $\deg(f_2) \leq d - 1$, then

$$|\mathsf{Z}(f_1, \ldots, f_r)| \leq (d-1)^2 q^{m-2}.$$

Proof. For $r = 2$ this follows directly from Theorem 2.2. Therefore we assume $r > 2$ from now on. To estimate $|\mathsf{Z}(f_1, \ldots, f_r)|$ we proceed as follows: Let p be an irreducible factor of f_1. Since we assume that $\gcd(f_1, \ldots, f_r) = 1$, there exists $i \geq 2$ such that $\gcd(p, f_i) = 1$. Using Theorem 2.2, we see that $|\mathsf{Z}(p, f_2, \ldots, f_r)| \leq |\mathsf{Z}(p, f_i)| \leq \deg(p) dq^{m-2}$. On the other hand if $f_1 = p_1 \cdots p_k$ for some irreducible, but not necessarily distinct, $p_1, \ldots, p_k \in T$, then $|\mathsf{Z}(f_1, \ldots, f_r)| \leq \sum_j |\mathsf{Z}(p_j, f_2, \ldots, f_r)|$. Combining these two estimates, we find that

$$|\mathsf{Z}(f_1, \ldots, f_r)| \leq \deg(f_1) dq^{m-2} \leq (d-1) dq^{m-2}.$$

Now suppose $\deg(f_1) \leq d-1$ and $\deg(f_2) \leq d-1$. Here, we need a more refined analysis. Let $g = \gcd(f_1, f_2)$ and write $b = \deg(g)$ and $f_1 = g f_1'$, $f_2 = g f_2'$. Since f_1 and f_2 are linearly independent, f_1' and f_2' are nonconstant polynomials. Hence $b < d-1$. It is clear that

$$|\mathsf{Z}(f_1, \ldots, f_r)| \leq |\mathsf{Z}(f_1', f_2')| + |\mathsf{Z}(g, f_3, \ldots, f_r)|.$$

By Theorem 2.2, we find that $|\mathsf{Z}(f_1', f_2')| \leq (d-b-1)^2 q^{m-2}$. To estimate $|\mathsf{Z}(g, f_3, \ldots, f_r)|$ we proceed on similar lines as before and obtain that

$$|\mathsf{Z}(g, f_3, \ldots, f_r)| \leq b dq^{m-2}.$$

Hence we see that

$$|\mathsf{Z}(f_1, f_2, f_3, \ldots, f_r)| \leq (d-b-1)^2 q^{m-2} + b dq^{m-2} = \left((d-1)^2 + b(b-d+2)\right) q^{m-2}.$$

Since $0 \leq b \leq d-2$, the maximal value of $b(b-d+2)$ is attained for $b = 0$ (or $b = d-2$). The conclusion of the lemma now follows in this case as well. □

We will also need the following result due to Homma and Kim [7, Thm.1.2]:

Theorem 2.4. *Let $\mathcal{X} \subset \mathbb{P}^m(\overline{\mathbb{F}}_q)$ be a hypersurface of degree d defined over $\mathbb{F}_q$ without an $\mathbb{F}_q$-linear component, and let $\mathcal{X}(\mathbb{F}_q)$ denote the set of its $\mathbb{F}_q$-rational points. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1) q^{m-1} + d q^{m-2} + p_{m-3}.$$

The following lemma will play an important role later and it appears, for example, in [11, Lem. 3.3]. See also [3, Lem. 2.1 and Rem. 2.3]. We outline a proof for the sake of completeness.

Lemma 2.5. *Let $\mathcal{X} \subseteq \mathbb{P}^m(\mathbb{F}_q)$ be any subset. Define*

$$a := \max_{\mathcal{H}} |\mathcal{X} \cap \mathcal{H}|,$$

where $\mathcal{H}$ ranges over all hyperplanes in $\mathbb{P}^m$ defined over $\mathbb{F}_q$. Then

$$|\mathcal{X}| \leq aq + 1 \quad \textit{and if } \mathcal{X} \neq \mathbb{P}^m(\mathbb{F}_q), \textit{ then } \quad |\mathcal{X}| \leq aq.$$

Proof. Let $\hat{\mathbb{P}}^m(\mathbb{F}_q)$ denotes the set of hyperplanes in $\mathbb{P}^m$ defined over $\mathbb{F}_q$. Counting the incidence set $\{(P, H) \in \mathcal{X} \times \hat{\mathbb{P}}^m(\mathbb{F}_q) : P \in H\}$ in two ways using the first and the second projections, we obtain $|\mathcal{X}| p_{m-1} \leq a p_m$. This gives $|\mathcal{X}| \leq aq + (a/p_{m-1}) \leq aq + 1$, since $a \leq p_{m-1}$. Further, if $a < p_{m-1}$, then $|\mathcal{X}| \leq aq$, since $|\mathcal{X}|$ is an integer, whereas if $a = p_{m-1}$ and $|\mathcal{X}| = aq + 1 = p_m$, then we must have $\mathcal{X} = \mathbb{P}^m(\mathbb{F}_q)$. This completes the proof. □

We have already alluded to an important result of Heijnen and Pellikaan [6]. We end this subsection by recording its statement essentially as in [6, Thm. 5.10], and then outline how the version stated in the Introduction can be deduced.

Theorem 2.6. *Assume that* $1 \le d < q$ *and* $r \le \binom{m+d}{d}$. *Then*

$$e_r^{\mathbb{A}}(d,m) = q^m - \Big(1 + \sum_{j=1}^{m} \alpha_j q^{m-j}\Big), \tag{8}$$

where $(\alpha_1, \ldots, \alpha_m)$ *is the* r^{th} *tuple in ascending lexicographic order among* m*-tuples* $(\lambda_1, \ldots, \lambda_m)$ *with coordinates from* $\{0, 1, \ldots, q-1\}$ *satisfying* $\lambda_1 + \cdots + \lambda_m \ge m(q-1) - d$,

To see the equivalence with (3), let us rewrite the expression on the right in (8) as

$$\sum_{j=1}^{m}(q^{m-j+1} - q^{m-j} - \alpha_j q^{m-j}) = \sum_{j=1}^{m} \beta_j q^{m-j}, \quad \text{where } \beta_j := q - 1 - \alpha_j \text{ for } j = 1, \ldots, m.$$

Note that $(\beta_1, \ldots, \beta_m)$ is precisely the rth tuple in descending lexicographic order among all m-tuples $\gamma = (\gamma_1, \ldots, \gamma_m)$ with coordinates in $\{0, 1, \ldots, q-1\}$ satisfying $\gamma_1 + \cdots + \gamma_m \le d$. Moreover, if $d < q$, then the last condition implies $\gamma_j \le q - 1$ for $j = 1, \ldots, m$. So if we take

$$\Sigma(d,m) := \{\gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbb{N}^m : \gamma_1 + \cdots + \gamma_m \le d\} \tag{9}$$

and β the rth element of $\Sigma(d,m)$ in descending lexicographic order, then (8) implies (3).

2.2 Combinatorics of $H_r(d,m)$

As mentioned in the Introduction, we are mainly interested in this paper in conjectural equality (7) and it is therefore important to understand $H_r(d,m)$ a little better. Let us begin by recalling the definition:

$$H_r(d,m) := \sum_{j=1}^{m} \beta_j q^{m-j}, \quad \text{for } m \ge 1,\ 1 \le d < q \text{ and } 1 \le r \le \tbinom{m+d}{d},$$

where β the rth element of $\Sigma(d,m)$ in descending lexicographic order and where $\Sigma(d,m)$ is as in (9). We shall now proceed to establish several elementary properties of $H_r(d,m)$. These might seem disparate at first, but they will turn out to be useful in later sections.

Observe that if $\lambda_1, \ldots, \lambda_m$ are integers, not all zero, with $|\lambda_j| \le q-1$ for $j = 1, \ldots, m$, then the sum $\sum_{j=1}^{m} \lambda_j q^{m-j}$ has the same sign as that of the first nonzero integer among $\lambda_1, \ldots, \lambda_m$. Now if $d < q$ and if $\gamma, \gamma' \in \Sigma(d,m)$, then using the above observation for $\lambda = \gamma - \gamma'$, we see that

$$\gamma <_{\text{lex}} \gamma' \iff \sum_{j=1}^{m} \gamma_j q^{m-j} \ < \ \sum_{j=1}^{m} \gamma'_j q^{m-j}.$$

This implies the strict monotonicity of $H_r(d,m)$ in the parameter r:

$$H_1(d,m) > H_2(d,m) > \cdots > H_{\binom{m+d}{d}}(d,m). \tag{10}$$

We will now try to determine $H_r(d.m)$ explicitly for "small" values of r. For $1 \le i \le m+1$, let $\mathbf{e}_i^m$ be the m-tuple with 1 in ith place and 0 elsewhere; when $i = m+1$, this is the zero-tuple. Clearly, the first $m+1$ elements of $\Sigma(d,m)$ are $(d-1)\mathbf{e}_1^m + \mathbf{e}_r^m$ for $r = 1, \ldots, m+1$. Consequently,

$$H_r(d,m) = (d-1)q^{m-1} + \lfloor q^{m-r} \rfloor \quad \text{for } 1 \le r \le m+1 \text{ and } 1 \le d < q. \tag{11}$$

In particular, if $d = 1$, then we have the simple expression $\lfloor q^{m-r} \rfloor$ for $H_r(d, m)$ for all permissible values of r. Now suppose $2 \le d < q$. Then the first $\binom{m+2}{2}$ elements can be described in blocks of $(m+1), m, (m-1), \ldots, 2, 1$ as follows

$$\begin{aligned}
&(d-2)\mathbf{e}_1^m + \mathbf{e}_1^m + \mathbf{e}_j^m \quad \text{for} \quad j = 1, \ldots, m+1,\\
&(d-2)\mathbf{e}_1^m + \mathbf{e}_2^m + \mathbf{e}_j^m \quad \text{for} \quad j = 2, \ldots, m+1,\\
&(d-2)\mathbf{e}_1^m + \mathbf{e}_3^m + \mathbf{e}_j^m \quad \text{for} \quad j = 3, \ldots, m+1,\\
&\quad \vdots\\
&(d-2)\mathbf{e}_1^m + \mathbf{e}_m^m + \mathbf{e}_j^m \quad \text{for} \quad j = m, m+1,\\
&(d-2)\mathbf{e}_1^m + \mathbf{e}_{m+1}^m + \mathbf{e}_{m+1}^m = (d-2)\mathbf{e}_1^m.
\end{aligned}$$

Put another way, for $r \le \binom{m+2}{2}$, the rth element of $\Sigma(d, m)$ is of the form

$$(d-2)\mathbf{e}_1^m + \mathbf{e}_i^m + \mathbf{e}_j^m \quad \text{for unique } i, j \in \mathbb{Z} \text{ with } 1 \le i \le j \le m+1. \tag{12}$$

An easy calculation shows that these unique i, j are related to $r \le \binom{m+2}{2}$ by:

$$r = (i-1)m - \tbinom{i-1}{2} + j \quad \text{and} \quad 1 \le i \le j \le m+1. \tag{13}$$

The conditions (13) determine i, j uniquely from a given $r \le \binom{m+2}{2}$. From (12), we see that

$$H_r(d, m) = (d-2)q^{m-1} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor \quad \text{for } r \le \tbinom{m+2}{2} \text{ with } i, j \text{ as in (13).} \tag{14}$$

Notice that in the above setting $i = 1$ if and only if $r \le m+1$ and in this case (14) simplifies to (11), at least when $d \ge 2$. As an additional illustration of (14), we may also note that

$$H_{m+2}(d, m) = (d-2)q^{m-1} + 2\lfloor q^{m-2} \rfloor \quad \text{for } 2 \le d < q. \tag{15}$$

Having observed that $H_r(d, m)$ is strictly monotonic in the parameter r, we will examine in the next two results the behavior of $H_r(d, m)$ as a function of the parameter d or the parameter m.

Proposition 2.7. *Assume that $1 < d < q$ and let c be an integer with $0 < c < d-1$. Then*

$$H_r(d, m) = cq^{m-1} + H_r(d-c, m) \quad \textit{for } 1 < r \le \tbinom{m+2}{2}. \tag{16}$$

In particular, $H_r(d-1, m) < H_r(d, m)$ whenever $2 < d < q$ and $1 < r \le \binom{m+2}{2}$.

Proof. Fix r with $1 < r \le \binom{m+2}{2}$, and let i, j be as in (13). Then $j \ge 2$. Also $1 < d - c < q$. Thus by (14), we see that $H_r(d, m) - H_r(d-c, m) = cq^{m-1}$. This implies the desired result. □

Proposition 2.8. *Assume that $1 \le d < q$ and $m > 1$. Then*

(i) $qH_r(d, m-1) \le H_r(d, m)$ whenever $1 \le r \le \binom{m+d-1}{d}$.

(ii) $qH_{r-1}(d, m-1) \le H_r(d, m)$ whenever $m+1 \le r \le \binom{m+d-1}{d}$.

Proof. Consider $\phi : \Sigma(d, m-1) \to \Sigma(d, m)$ defined by $\phi(\gamma_1, \ldots, \gamma_{m-1}) = (\gamma_1, \ldots, \gamma_{m-1}, 0)$. It is clear that ϕ preserves lexicographic order and that it maps the first $m-1$ elements of $\Sigma(d, m-1)$ to the first $m-1$ elements of $\Sigma(d, m)$. Thus if β is the rth element of $\Sigma(d, m-1)$, then $\phi(\beta)$ is the sth element of $\Sigma(d, m)$ for some $s \ge r$. Hence in view of (10), we find, for $r \le \binom{m+d-1}{d}$,

$$qH_r(d, m-1) = q\sum_{j=1}^{m-1} \beta_j q^{m-1-j} = \sum_{j=1}^{m} \phi(\beta)_j q^{m-j} = H_s(d, m) \le H_r(d, m). \tag{17}$$

This proves (i). Next, observe that the image of ϕ misses the mth element of $\Sigma(d,m)$, namely, $(d-1,0,\ldots,0,1)$. It follows that if $r-1 \geq m$ and if γ is the $(r-1)$th element of $\Sigma(d,m-1)$, then $\phi(\gamma)$ is the sth element of $\Sigma(d,m)$ for some $s \geq r = (r-1)+1$. Thus as in (17), we see that $qH_{r-1}(d,m-1) \leq H_r(d,m)$ whenever $m+1 \leq r \leq \binom{m+d-1}{d}$. This proves (ii). □

2.3 Projective Varieties containing a Hyperplane and Zanella's Theorem for Quadrics

The following result about projective varieties containing a hyperplane is a slightly more general version of [4, Lem. 2.5]. We include a quick proof for the sake of completeness.

Lemma 2.9. *Assume that $d \leq q$. Let $F_1,\ldots,F_r$ be linearly independent homogeneous polynomials in S_d. Suppose that $L \in S_1$ divides each of $F_1,\ldots,F_r$. Then*

$$|\mathsf{V}(F_1,\ldots,F_r)| \leq H_r(d-1,m) + p_{m-1}.$$

Proof. The conditions on L show that L is nonzero and thus without loss of generality, we may assume that $L = X_0$. For $1 \leq i \leq m$, let $f_i(X_1,\ldots,X_m) := F_i(1,X_1,\ldots,X_m)$; note that $\deg(f_i) \leq d-1$, since $X_0 \mid F_i$. Hence (3) implies that $|\mathsf{Z}(f_1,\ldots,f_r)| \leq H_r(d-1,m)$, and so

$$|\mathsf{V}(F_1,\ldots,F_r)| = |\mathsf{Z}(f_1,\ldots,f_r)| + |\mathsf{V}(X_0)| \leq H_r(d-1,m) + p_{m-1},$$

as desired. □

Note that for the hypothesis of Lemma 2.9 to hold, it is necessary that $r \leq \binom{m+d-1}{d-1}$, because otherwise the polynomials $F_1,\ldots,F_r$ cannot be linearly independent. Indeed, by assumption, the polynomials $F_1,\ldots,F_r$ are in the vector space $L \cdot S_{d-1}$, which has dimension $\binom{m+d-1}{d-1}$.

The last preliminary result we need is the following theorem of Zanella [11, Thm. 3.4] about maximum possible number of $\mathbb{F}_q$-rational points on intersections of r linearly independent quadrics in $\mathbb{P}^m$.

Theorem 2.10. *Assume that $r \leq \binom{m+2}{2}$. Let k be the unique integer such that $-1 \leq k < m$ and $\binom{m+2}{2} - \binom{k+3}{2} < r \leq \binom{m+2}{2} - \binom{k+2}{2}$. Then*

$$e_r(2,m) = \lfloor q^{\binom{m+2}{2}-\binom{k+2}{2}-r-1} \rfloor + p_k.$$

In particular, if $r \leq m+1$, then $k = m-1$ and thus $e_r(2,m) = \lfloor q^{m-r} \rfloor + p_{m-1}$.

We have now gathered all known results from the literature that we need. We finish this section by restating the following conjecture from [4], which was alluded to in the Introduction.

Conjecture 1. *Assume that $1 < d < q$ and $1 \leq r \leq \binom{m+d-1}{d-1}$. Then*

$$e_r(d,m) = H_r(d-1,m) + p_{m-1}.$$

This conjecture was proved to be correct for $r \leq m+1$ and $d < q-1$ in [4]. For $r = 1$, the conjecture follows from Theorem 2.1, whereas for $d = 2$, it follows as a particular case of Theorem 2.10 [in view of (11)], or alternatively, as a special case of [4, Thm. 6.3]. Also when $m = 1$, the conjecture is a trivial consequence of (5). Based on the above, we may always assume that $m > 1$, $r > 1$, and $d \geq 3$. We will provide significant more evidence for this conjecture by proving it for any pair (d,r) satisfying $2 < d < q$ and $r \leq \binom{m+2}{2}$. In particular, we show that

the conjecture holds if $d = 3$. The main step in our proof would be to show if $r \leq \binom{m+2}{2}$ and if $F_1, \ldots, F_r$ are any linearly independent polynomials in S_d, then

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq H_r(d-1, m) + p_{m-1}. \tag{18}$$

The equality in Conjecture 1 is established by using (3) to show that there exists a family of polynomials where the upper the bound in (18) is attained.

3 Reduction to the relatively prime case

In order to prove (18) for any linearly independent $F_1, \ldots, F_r \in S_d$, we will establish in this section auxiliary results that deal with the case when $\gcd(F_1, \ldots, F_r)$ has degree $c > 1$. Since (18) is known already when $r = 1$, we will usually assume that $r > 1$. Note that when $r > 1$, the linear independence of $F_1, \ldots, F_r$ implies that $c < d$.

Lemma 3.1. *Assume that $r > 1$ and $1 < d \leq q$. Let $F_1, \ldots, F_r \in S_d$ be linearly independent and G be a gcd of $F_1, \ldots, F_r$ and let $c := \deg G$. Let $F_1', \ldots, F_r' \in S_{d-c}$ be such that $F_i = GF_i'$ for $i = 1, \ldots, r$. Suppose $c > 0$ and G has no linear factors. Then*

$$|\mathsf{V}(F_1, \ldots, F_r)| < cq^{m-1} + |\mathsf{V}(F_1', \ldots, F_r')|.$$

Proof. Since $r > 1$, we must have $c < d$ and so $c \leq q - 1$. Hence using Theorem 2.4, we obtain

$$|\mathsf{V}(G)| \leq (c-1)q^{m-1} + cq^{m-2} + p_{m-3} < cq^{m-1}.$$

Since we clearly have $|\mathsf{V}(F_1, \ldots, F_r)| \leq |\mathsf{V}(G)| + |\mathsf{V}(F_1', \ldots, F_r')|$, the lemma follows. □

Similar to the remark after Lemma 2.9, one can deduce that if G and c are as in Lemma 3.1, then we necessarily have $r \leq \binom{m+d-c}{d-c}$, since $F_1, \ldots, F_r \in G \cdot S_{d-c}$. This gives an alternative argument to show that if $r > 1$, then $c < d$.

Proposition 3.2. *Assume that $1 < r \leq \binom{m+2}{2}$ and $2 < d \leq q$. Let $F_1, \ldots, F_r \in S_d$ be linearly independent and G be a gcd of $F_1, \ldots, F_r$ and let $c := \deg G$. Let $F_1', \ldots, F_r' \in S_{d-c}$ be such that $F_i = GF_i'$ for $i = 1, \ldots, r$. If $0 < c < d - 2$ and $|\mathsf{V}(F_1', \ldots, F_r')| \leq H_r(d-c-1, m) + p_{m-1}$, then*

$$|\mathsf{V}(F_1, \ldots, F_r)| < H_r(d-1, m) + p_{m-1}.$$

Proof. If G contains a linear factor and in particular, if $c = 1$, then the result follows from Lemma 2.9. Now suppose G has no linear factors, $1 < c < d - 2$, and $|\mathsf{V}(F_1', \ldots, F_r')| \leq H_r(d-c-1, m) + p_{m-1}$. By Lemma 3.1, we see that

$$|\mathsf{V}(F_1, \ldots, F_r)| < cq^{m-1} + H_r(d-c-1, m) + p_{m-1}.$$

On the other hand, changing d to $d-1$ in (16), we find $H_r(d-1, m) = cq^{m-1} + H_r(d-c-1, m)$. This yields the desired inequality. □

The cases $c = d-2$ and $c = d-1$ that are not covered by Proposition 3.2 need to be dealt with independently. However, since the values of $e_r(1, m)$ and $e_r(2, m)$ are known for all permissible values of r, this is not hard to do.

Proposition 3.3. *Assume that $1 < r \leq \binom{m+2}{2}$ and $2 < d \leq q$. Let $F_1, \ldots, F_r \in S_d$ be linearly independent and let G be a gcd of $F_1, \ldots, F_r$. Suppose $c := \deg G$ equals $d - 2$ or $d - 1$. Then*

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq H_r(d-1, m) + p_{m-1}.$$

Proof. If G contains a linear factor, then Lemma 2.9 gives the desired result. Now assume that G has no linear factors. Then Theorem 2.4 implies that

$$|\mathsf{V}(G)| \leq (c-1)q^{m-1} + cq^{m-2} + p_{m-3}.$$

As in the previous proposition, let $F_1', \ldots, F_r' \in S_{d-c}$ be such that $F_i = GF_i'$ for $i = 1, \ldots, r$. Then $|\mathsf{V}(F_1, \ldots, F_r)| \leq |\mathsf{V}(G)| + |\mathsf{V}(F_1', \ldots, F_r')|$. Consequently,

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq (c-1)q^{m-1} + cq^{m-2} + p_{m-3} + e_r(d-c, m). \tag{19}$$

First, let us suppose $c = d-1$. Then we necessarily have $1 < r \leq m+1$. Also in view of (5), $e_r(1, m) = p_{m-r} \leq p_{m-2}$. Thus (19) implies that

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq (d-2)q^{m-1} + (d-1)q^{m-2} + p_{m-3} + p_{m-2}.$$

Since $d \leq q$, we see that the expression on the right-hand side of the above inequality is strictly smaller than $(d-2)q^{m-1} + p_{m-1}$. Hence in view of (11) and (10), we see that

$$|\mathsf{V}(F_1, \ldots, F_r)| < (d-2)q^{m-1} + p_{m-1} = H_{m+1}(d-1, m) + p_{m-1} \leq H_r(d-1, m) + p_{m-1},$$

as desired. Next, let us suppose $c = d-2$. Then by Theorem 2.10, we see that

$$e_r(2, m) = \lfloor q^{m-r} \rfloor + p_{m-1} \leq q^{m-2} + p_{m-1} \quad \text{if } 1 < r \leq m+1,$$

whereas

$$e_r(2, m) \leq e_{m+2}(2, m) = \lfloor q^{m-2} \rfloor + p_{m-2} \quad \text{if } \ m+1 < r \leq \binom{m+2}{2}.$$

Using this together with (19) and the assumption that $d \leq q$, we see that for $1 < r \leq m+1$,

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq (d-3)q^{m-1} + (d-2)q^{m-2} + p_{m-3} + q^{m-2} + p_{m-1} < (d-2)q^{m-1} + p_{m-1},$$

and thus in view of (10), we find $|\mathsf{V}(F_1, \ldots, F_r)| \leq H_{m+1}(d-1, m) + p_{m-1} \leq H_r(d-1, m) + p_{m-1}$. Likewise, when $m+1 < r \leq \binom{m+2}{2}$, from (19) and the assumption $d \leq q$ we obtain

$$|\mathsf{V}(F_1, \ldots, F_r)| \leq (d-3)q^{m-1} + (d-2)q^{m-2} + p_{m-3} + \lfloor q^{m-2} \rfloor + p_{m-2} < (d-3)q^{m-1} + p_{m-1}.$$

In view of (14), the expression on the right is $H_{\binom{m+2}{2}}(d-1, m) + p_{m-1}$, which, thanks to (10), is less than or equal to $H_r(d-1, m) + p_{m-1}$. This completes the proof. □

4 The relatively prime case

In this section, we will establish results that help in proving (18) when the polynomials $F_1, \ldots, F_r$ are relatively prime. Note that for any linearly independent $F_1, \ldots, F_r \in S_d$, the corresponding projective variety $\mathsf{V}(F_1, \ldots, F_r)$ coincides with $\mathsf{V}(W)$, where W is the $\mathbb{F}_q$-linear subspace of S_d spanned by $F_1, \ldots, F_r$. Moreover, we can replace $F_1, \ldots, F_r$ by any other basis of W. We will thus focus on estimating $|\mathsf{V}(W)|$, where W is any r-dimensional subspace of S_d and take $F_1, \ldots, F_r$ to be judiciously chosen basis elements of W. To this end, an important role will be played by an integer, that we call the *t-invariant* of the subspace W, which is essentially the largest dimension of the space of polynomials in W that are divisible by a linear homogeneous polynomial. More precisely, given any subspace $W \subseteq S_d$ and $0 \neq L \in S_1$, we define $t_W(L) := \dim(W \cap LS_{d-1})$. Note that $0 \leq t_W(L) \leq \dim W$. The *t-invariant* of W is defined by

$$t_W := \max\{t_W(L) : L \in S_1, \ L \neq 0\}.$$

Clearly, $0 \le t_W \le \dim W$. Moreover, if $t_W = \dim W = r$, then there exists $0 \neq L \in S_1$ such that L divides every element of W. In particular, if W is spanned by linearly independent $F_1, \ldots, F_r \in S_d$ that are relatively prime, then $t_W < r$. Conversely, if $t_W < r = \dim W$, then for any $F_1, \ldots, F_r \in S_d$ that form a basis of W, the polynomials $F_1, \ldots, F_r$ do not have a common linear factor, or in other words, $\mathsf{V}(F_1, \ldots, F_r)$ does not contain a hyperplane.

Context

In this section, we will always assume that $2 < d < q$ and $m > 1$. Assumption on r may vary and will be specified.

Our first lemma gives a basic set of inequalities that hold under the hypothesis that the inequality (18), which we wish to prove, holds when m is replaced by $m-1$.

Lemma 4.1. *Assume that* $1 < r \le \binom{m+d-1}{d-1}$. *Suppose*

$$e_s(d, m-1) \le H_s(d-1, m-1) + p_{m-2} \quad \text{for} \quad 1 \le s < r. \tag{20}$$

Then for any r*-dimensional subspace* W *of* S_d *with* $t := t_W$ *satisfying* $1 \le t < r$, *we have*

$$|\mathsf{V}(W)| \le H_{r-t}(d-1, m-1) + p_{m-2} + H_t(d-1, m). \tag{21}$$

Moreover, if $t = 1$, *then*

$$|\mathsf{V}(W)| \le H_{r-1}(d-1, m-1) + p_{m-2} + d(d-1)q^{m-2}, \tag{22}$$

whereas if $t \ge 2$, *then*

$$|\mathsf{V}(W)| \le H_{r-t}(d-1, m-1) + p_{m-2} + (d-1)^2 q^{m-2}. \tag{23}$$

Proof. Let W be any r-dimensional subspace W of S_d with $t := t_W < r$. By a linear change of coordinates, we can and will assume that $t = t_W(X_0)$. Now we can choose a basis $\{F_1, \ldots, F_r\}$ of W such that $\{F_1, \ldots, F_t\}$ is a basis of $W \cap X_0 S_{d-1}$. Let $F_1', \ldots, F_t' \in S_{d-1}$ be such that $F_i = X_0 F_i'$ for $i = 1, \ldots, t$. Also let $f_1, \ldots, f_r$ denote, respectively, the polynomials in T obtained by putting $X_0 = 1$ in $F_1, \ldots, F_r$. Note that $\deg f_i \le d-1$ for $i = 1, \ldots, t$ and $\deg f_i \le d$ for $i = t+1, \ldots, r$. Intersecting $\mathsf{V}(W)$ with the hyperplane $\mathsf{V}(X_0)$ and its complement, we obtain

$$|\mathsf{V}(W)| = |\mathsf{V}(F_{t+1}, \ldots, F_r) \cap \mathsf{V}(X_0)| + |\mathsf{Z}(f_1, \ldots, f_r)| \le e_{r-t}(d, m-1) + |\mathsf{Z}(f_1, \ldots, f_r)|.$$

Consequently, (21) follows from (20) and (3), since $|\mathsf{Z}(f_1, \ldots, f_r)| \le |\mathsf{Z}(f_1, \ldots, f_t)|$. Moreover, (22) and (23) are easily deduced from the inequality displayed above and Lemma 2.3. □

We shall now proceed to refine the inequalities in (21)–(23) into (18) by considering separately various possibilities for the t-invariant of a given subspace of S_d. It will be seen that in many cases we obtain a strict inequality.

Lemma 4.2. *Assume that* $1 < r \le m+1$. *Also suppose* (20) *holds. Let* W *be an* r*-dimensional subspace of* S_d *satisfying* $t_W = 1$. *Then* $|\mathsf{V}(W)| < H_r(d-1, m) + p_{m-1}$.

Proof. By Lemma 4.1, we see that (22) holds. This together with (11) gives

$$\begin{aligned}
|\mathsf{V}(W)| &\le H_{r-1}(d-1, m-1) + p_{m-2} + d(d-1)q^{m-2} \\
&= (d-2)q^{m-2} + \lfloor q^{m-r} \rfloor + p_{m-2} + d(d-1)q^{m-2} \\
&\le (d-2)q^{m-2} + \lfloor q^{m-r} \rfloor + p_{m-2} + (q-1)(d-2)q^{m-2} + (q-1)q^{m-2} \\
&= (d-2)q^{m-1} + \lfloor q^{m-r} \rfloor + p_{m-1} - q^{m-2} \\
&< H_r(d-1, m) + p_{m-1},
\end{aligned}$$

where the last inequality uses (11) and the assumption that $m \ge 2$. □

Lemma 4.3. *Assume that* $1 < r \le m+1$. *Also suppose* (20) *holds. Let* W *be any* r*-dimensional subspace of* S_d *satisfying* $2 \le t_W < r$. *Then* $|\mathsf{V}(W)| < H_r(d-1,m) + p_{m-1}$.

Proof. Let $t := t_W$. By Lemma 4.1, we see that $|\mathsf{V}(W)| \le H_{r-t}(d-1,m-1)+p_{m-2}+H_t(d-1,m)$. Now since $t \le m$ and $r-t \le m-1$, we see from (11) that

$$|\mathsf{V}(W)| \le (d-2)q^{m-2} + q^{(m-1)-(r-t)} + p_{m-2} + (d-2)q^{m-1} + q^{m-t}.$$

Further, since $2 \le t < r$, we find $(m-1)-(r-t) \le m-2$ and $m-t \le m-2$. Consequently, $q^{(m-1)-(r-t)} + q^{m-t} \le 2q^{m-2}$. Thus the above estimate simplifies to

$$|\mathsf{V}(W)| \le dq^{m-2} + (d-2)q^{m-1} + p_{m-2} \le (d-2)q^{m-1} + p_{m-1} - q^{m-2} < (d-2)q^{m-1} + p_{m-1},$$

where the second inequality uses $d \le q-1$. Also $H_r(d-1,m) = (d-2)q^{m-1} + \lfloor q^{m-r} \rfloor$, thanks to (11). Thus $(d-2)q^{m-1} \le H_r(d-1,m)$, which yields $|\mathsf{V}(W)| < H_r(d-1,m) + p_{m-1}$. □

Lemma 4.4. *Assume that* $m+1 < r \le \binom{m+2}{2}$. *Also suppose* (20) *holds. Let* W *be any* r*-dimensional subspace of* S_d *satisfying* $2 \le t_W \le m+1$. *Then* $|\mathsf{V}(W)| \le H_r(d-1,m) + p_{m-1}$.

Proof. Let $t := t_W$. By Lemma 4.1, we see that (23) holds. In view of (10), this gives

$$|\mathsf{V}(W)| \le H_{r-t}(d-1,m-1)+p_{m-2}+(d-1)^2q^{m-2} \le H_{r-(m+1)}(d-1,m-1)+p_{m-2}+(d-1)^2q^{m-2}.$$

Now since $m+1 < r \le \binom{m+2}{2}$, there are unique $i,j \in \mathbb{Z}$ satisfying conditions as in (13), namely,

$$r = (i-1)m - \binom{i-1}{2} + j \quad \text{and} \quad 2 \le i \le j \le m+1.$$

This implies that an equation for $r-(m+1)$ such as (13) with m changed to $m-1$, is given by

$$r-(m+1) = (i-2)(m-1) - \binom{i-2}{2} + (j-1) \quad \text{and} \quad 1 \le (i-1) \le (j-1) \le m.$$

Thus using (14), we see that $H_r(d-1,m) = (d-3)q^{m-1} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor$ and moreover,

$$H_{r-(m+1)}(d-1,m-1) = (d-3)q^{m-2} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor,$$

where we note that $H_{r-(m+1)}(d-1,m-1)$ is well-defined since $r-(m+1) \le \binom{m+1}{2} \le \binom{m+d-2}{d-1}$, thanks to our assumptions on d,m and r. Using this in the above estimate for $|\mathsf{V}(W)|$, we obtain

$$\begin{aligned}
|\mathsf{V}(W)| &\le (d-3)q^{m-2} + p_{m-2} + (d-1)^2q^{m-2} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor \\
&= (d-2)(d+1)q^{m-2} + p_{m-2} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor \\
&\le (d-2)q^{m-1} + p_{m-2} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor \\
&= (d-3)q^{m-1} + p_{m-1} + \lfloor q^{m-i} \rfloor + \lfloor q^{m-j} \rfloor \\
&= H_r(d-1,m) + p_{m-1},
\end{aligned}$$

where the second inequality above uses the assumption that $d \le q-1$. □

Lemma 4.5. *Assume that* $m+1 < r \le \binom{m+2}{2}$. *Also suppose* (20) *holds. Let* W *be any* r*-dimensional subspace of* S_d *satisfying* $m+1 < t_W < r$. *Then* $|\mathsf{V}(W)| \le H_r(d-1,m) + p_{m-1}$.

Proof. Let $t := t_W$. By Lemma 4.1, we see that $|\mathsf{V}(W)| \le H_{r-t}(d-1,m-1)+p_{m-2}+H_t(d-1,m)$. Here $t \ge m+2$ and $r-t \ge 1$. Hence from (10), we see that

$$|\mathsf{V}(W)| \le H_1(d-1,m-1) + p_{m-2} + H_{m+2}(d-1,m).$$

Consequently, using (11) and (15), we obtain

$$\begin{aligned} |\mathsf{V}(W)| &\le (d-2)q^{m-2} + \lfloor q^{m-2} \rfloor + p_{m-2} + (d-3)q^{m-1} + 2\lfloor q^{m-2} \rfloor \\ &= (d-3)q^{m-1} + (d+1)q^{m-2} + p_{m-2}. \end{aligned}$$

Since $d \le q-1$, this gives $|\mathsf{V}(W)| \le (d-3)q^{m-1} + p_{m-1}$, and so in view of (14), we conclude that $|\mathsf{V}(W)| \le H_r(d-1,m) + p_{m-1}$. □

It remains to prove (18) when $t_W = 0$ and also when $t_W = 1$ and $m+1 < r \le \binom{m+2}{2}$. Here we need a slightly different technique.

Lemma 4.6. *Assume that* $1 < r \le \binom{m+2}{2}$. *Also suppose* (20) *holds. Let* W *be any* r*-dimensional subspace of* S_d *satisfying either (i)* $t_W = 0$ *or (ii)* $t_W = 1$ *and* $m+1 < r \le \binom{m+2}{2}$. *Then* $|\mathsf{V}(W)| \le H_r(d-1,m) + p_{m-1}$.

Proof. Let $t := t_W$. Given any hyperplane $\mathcal{H}$ in $\mathbb{P}^m$, we have $\mathcal{H} = \mathsf{V}(L)$ for some $0 \ne L \in S_1$. Now $t_W(L) := \dim(W \cap LS_{d-1}) \le t$, and hence in view of (20) and (10), we see that

$$|\mathsf{V}(W) \cap \mathcal{H}| \le e_{r-t_W(L)}(d-1,m-1) \le H_{r-t_W(L)}(d-1,m-1)+p_{m-2} \le H_{r-t}(d-1,m-1)+p_{m-2}.$$

Since $\mathcal{H}$ was an arbitrary hyperplane in $\mathbb{P}^m$, using Lemma 2.5, we obtain

$$|\mathsf{V}(W)| \le q\left(H_{r-t}(d-1,m-1) + p_{m-2}\right) + 1 = qH_{r-t}(d-1,m-1) + p_{m-1}.$$

Hence the desired result follows from parts (i) and (ii) of Proposition 2.8. □

5 Completion of the Proof

In this section we combine the results of the previous sections to prove one of our main results.

Context

As before, d, m, r are fixed positive integers. As in Conjecture 1, we generally assume that $1 < d < q$. But the relevant assumptions are specified in the statement of the results.

Lemma 5.1. *Assume that* $2 < d < q$ *and* $1 \le r \le \binom{m+2}{2}$. *Then* (18) *holds, that is,*

$$|\mathsf{V}(F_1,\ldots,F_r)| \le H_r(d-1,m) + p_{m-1} \quad \textit{for any linearly independent } F_1,\ldots,F_r \in S_d.$$

Proof. We use induction on $d+m$. Note that since $d \ge 3$ and $m \ge 1$, we have $d+m \ge 4$ and if $d+m=4$, then $d=3$ and $m=1$, in which case (18) clearly holds, thanks to (5). Now assume that $d+m > 4$ and that (18) holds for smaller values of $d+m$. Since (18) follows from (5) when $m=1$ and from Theorem 2.1 when $r=1$, we shall henceforth assume that $m>1$ and $r>1$.

Let $F_1,\ldots,F_r$ be any linearly independent polynomials in S_d. Two cases are possible.

Case 1. $F_1,\ldots,F_r$ are not relatively prime, i.e., they have a nonconstant common factor.

In this case, the hypothesis of Proposition 3.2 is satisfied, thanks to the induction hypothesis. Thus from Propositions 3.2 and 3.3, we see that (18) holds.

Case 2. $F_1, \ldots, F_r$ are relatively prime.

In this case, (20) is satisfied, thanks to the induction hypothesis. Further if we let W be the subspace of S_d spanned by $F_1, \ldots, F_r$ and let $t = t_W$, then we have $0 \le t < r$. Hence from Lemmas 4.3, 4.4, and 4.5, we see that (18) holds when $t \ge 2$, whereas from Lemmas 4.2, and 4.6, we see that (18) holds when $t \le 1$. This completes the proof. □

The reverse inequality is easy to deduce from the Heijnen-Pellikaan Theorem.

Lemma 5.2. *Assume that* $1 < d \le q$ *and* $1 \le r \le \binom{m+d-1}{d-1}$. *Then*

$$e_r(d, m) \ge H_r(d-1, m) + p_{m-1}.$$

Proof. Note that $1 \le d-1 < q$ and hence by (3), there exist linearly independent $f_1, \ldots, f_r$ in $T_{\le d-1}$ such that $|\mathsf{Z}(f_1, \ldots, f_r)| = H_r(d-1, m)$. For $1 \le i \le r$, let $F_i' := X_0^{d-1} f_i(X_1/X_0, \ldots, X_m/X_0)$ and let $F_i := X_0 F_i'$. It is easily seen that $F_1, \ldots, F_r$ are linearly independent elements of S_d and that $e_r(d, m) \ge |\mathsf{V}(F_1, \ldots, F_r)| = H_r(d-1, m) + p_{m-1}$. □

Theorem 5.3. *Assume that* $1 < d < q$ *and* $1 \le r \le \binom{m+2}{2}$. *Then* $e_r(d, m) = H_r(d-1, m) + p_{m-1}$.

Proof. If $d = 2$, then the desired result follows from Theorem 2.10 as noted in the last paragraph of Section 2. If $d > 2$, then it is easily seen that $\binom{m+2}{2} \le \binom{m+d-1}{d-1}$, and so in this case the desired result follows from Lemmas 5.1 and 5.2. □

6 The case $d = q$

It may have been noted that several of the lemmas and propositions in previous sections are actually valid for $d = q$. Thus one may wonder if Conjecture 1 actually holds for $d = q$ as well. We will answer this here by showing that a straightforward analogue of Conjecture 1 is not valid for $d = q$, in general. More precisely, we will determine $e_r(q, m)$ for $1 \le r \le m+1$ and show that

$$e_r(q, m) > H_r(q-1, m) + p_{m-1} = (q-2)q^{m-1} + q^{m-r} + p_{m-1} \quad \text{when } q > 2 \text{ and } 1 < r \le m.$$

Note that the case $d = q = 2$ is already covered by Theorem 2.10, and here $e_r(q, m)$ behaves as in Conjecture 1. Likewise, when $d = q$ and $r = 1$, thanks to Theorem 2.1.

Lemma 6.1. *Assume that* $1 \le r \le m$. *Then*

$$e_r(q, m) \ge q^m + p_{m-r-1}.$$

Proof. For $1 \le i \le r$, consider $F_i \in S_q$ defined by $F_i := X_i^q - X_0^{q-1} X_i$. Clearly, $F_1, \ldots, F_r$ are linearly independent. Writing $\mathcal{X} = \mathsf{V}(F_1, \ldots, F_r)$ and $\mathcal{H} = \mathsf{V}(X_0)$, we see that

$$|\mathcal{X} \cap \mathcal{H}| = |\mathsf{V}(X_0, X_1^q, \ldots, X_r^q)| = |\{(a_0 : a_1 : \cdots : a_m) \in \mathbb{P}^m : a_i = 0 \text{ for } 0 \le i \le r\}| = p_{m-r-1}$$

and

$$|\mathcal{X} \cap \mathcal{H}^c| = |\mathsf{Z}(X_1^q - X_1, \ldots, X_m^q - X_m)| = q^m,$$

where $\mathcal{H}^c$ denotes the complement of $\mathcal{H}$ in $\mathbb{P}^m$. Thus $e_r(q, m) \ge |\mathcal{X}| = q^m + p_{m-r-1}$. □

We shall now show that the lower bound in Lemma 6.1 is, in fact, the exact value of $e_r(q, m)$ when $q \ge 3$. The technique used will be similar to that used in the proof of Theorem 5.3.

Theorem 6.2. *Assume that $q \geq 3$ and $1 \leq r \leq m$. Then*

$$e_r(q,m) = q^m + p_{m-r-1}.$$

Proof. In view of Lemma 6.1, it suffices to show that

$$e_r(q,m) \leq q^m + p_{m-r-1} \quad \text{for} \quad 1 \leq r \leq m. \tag{24}$$

We will prove this using induction on m. If $m = 1$, then (24) is an immediate consequence of (5). Now assume that $m > 1$ and that (24) holds for smaller values of m. Let $F_1, \ldots, F_r \in S_d$ be any linearly independent polynomials, spanning a linear space W. We write $t = t_W$ and without loss of generality, we may assume that $t_W = t_W(X_0)$ and also that $X_0 \mid F_i$ for $1 \leq i \leq t$. We shall write $\mathcal{X} = \mathsf{V}(F_1, \ldots, F_r)$ and $\mathcal{H} = \mathsf{V}(X_0)$, and divide the proof into two cases as follows.

Case 1: $t = 0$.

Here, using the induction hypothesis and the definition of t, we see that

$$|\mathcal{X} \cap \mathcal{H}'| \leq q^{m-1} + p_{(m-1)-r-1} \quad \text{for every hyperplane } \mathcal{H}' \text{ in } \mathbb{P}^m \text{ defined over } \mathbb{F}_q.$$

Hence from Lemma 2.5, we obtain (24).

Case 2: $1 \leq t \leq r$.

In this case using the induction hypothesis, we obtain

$$|\mathcal{X} \cap \mathcal{H}| \leq q^{m-1} + p_{(m-1)-(r-t)-1}$$

and since $t \leq r \leq m$ and $2 \leq (q-1) < q$, from (3) and (11), we obtain

$$|\mathcal{X} \cap \mathcal{H}^c| \leq |\mathsf{Z}(f_1, \ldots, f_t)| \leq H_t(q-1,m) = (q-2)q^{m-1} + q^{m-t},$$

where $\mathcal{H}^c$ denote the complement of $\mathcal{H} = \mathsf{V}(X_0)$ in $\mathbb{P}^m$. Therefore we have

$$|\mathcal{X}| \leq p_{m-r+t-2} + (q-1)q^{m-1} + q^{m-t} = q^m + p_{m-r-1} + R,$$

where

$$R = p_{m-r+t-2} - p_{m-r-1} - q^{m-1} + q^{m-t} = \frac{(q^{t-1}-1)\left(q^{m-r} - q^{m-t+1} + q^{m-t}\right)}{(q-1)} \leq 0,$$

where the last inequality follows since $m - r \leq m - t$ and $q \geq 2$. This proves (24). □

A special case of Theorem 6.2 is that if $q > 2$, then $e_1(q,m) = q^m + p_{m-2}$, and from (11), we see that this equals $H_1(q-1,m) + p_{m-1}$. However, when $q > 2$ and $1 < r \leq m$, by substituting $p_{m-r-1} = (q^{m-r}-1)/(q-1)$ and $p_{m-1} = (q^m-1)/(q-1)$, an elementary calculation shows that

$$(q^m + p_{m-r-1}) - (q-2)q^{m-1} - q^{m-r} - p_{m-1} = \frac{(q-2)\left(q^{m-1} - q^{m-r}\right)}{(q-1)} > 0,$$

and so $e_r(q,m) > H_r(q-1,m) + p_{m-1}$. Thus, Conjecture 1 does not hold for $d = q$ in general. Perhaps somewhat surprisingly, it turns out that Conjecture 1 is valid when $r = m+1$ and $d = q$. The proof follows a very similar pattern as in Theorem 6.2

Theorem 6.3. *Assume that $q \geq 3$. Then*

$$e_{m+1}(q,m) = (q-1)q^{m-1} + p_{m-2}.$$

Proof. We will show using induction on m that $e_{m+1}(q,m) \leq (q-1)q^{m-1} + p_{m-2}$. When $m = 1$, this follows from (5). Assume that $m > 1$ and that the inequality holds for smaller values of m. Let $F_1, \ldots, F_{m+1}$ be any linearly independent polynomials in S_q, and let W be the linear space spanned by them. Write $t = t_W$ and assume without loss of generality that $t = t_W(X_0)$ and also that $X_0 \mid F_i$ for $1 \leq i \leq t$. We shall write $\mathcal{X} = \mathsf{V}(F_1, \ldots, F_r)$ and $\mathcal{H} = \mathsf{V}(X_0)$, and divide the proof into two cases as follows.

Case 1: $t = 0$ or $t = 1$.

Using the induction hypothesis, we obtain for any hyperplane $\mathcal{H}'$ in $\mathbb{P}^m$ defined over $\mathbb{F}_q$,

$$|\mathcal{X} \cap \mathcal{H}'| \leq |\mathsf{V}(F_2, \ldots, F_{m+1}) \cap \mathcal{H}'| \leq (q-1)q^{m-2} + p_{(m-1)-2}.$$

Hence using Lemma 2.5 we obtain $|\mathcal{X}| \leq (q-1)q^{m-1} + p_{m-2}$.

Case 2: $2 \leq t \leq m+1$.

Here, we can apply Theorem 6.2 and it gives

$$|\mathcal{X} \cap \mathcal{H}| \leq q^{m-1} + p_{(m-1)-(m+1-t)-1} = q^{m-1} + p_{t-3}.$$

Moreover, using (3) and (11), we obtain

$$|\mathcal{X} \cap \mathcal{H}^c| \leq |\mathsf{Z}(f_1, \ldots, f_t)| \leq H_t(q-1, m) = (q-2)q^{m-1} + \lfloor q^{m-t} \rfloor,$$

where $f_i \in T_{\leq m}$ is obtained by putting $X_0 = 1$ in F_i for $1 \leq i \leq t$ and $\mathcal{H}^c = \mathbb{P}^m \setminus \mathcal{H}$. Hence

$$|\mathcal{X}| \leq q^{m-1} + p_{t-3} + (q-2)q^{m-1} + \lfloor q^{m-t} \rfloor = (q-1)q^{m-1} + p_{t-3} + \lfloor q^{m-t} \rfloor.$$

Since $2 \leq t \leq m+1$, this implies $|\mathcal{X}| \leq (q-1)q^{m-1} + p_{m-2}$.

It follows that $e_{m+1}(q,m) \leq (q-1)q^{m-1} + p_{m-2}$. The reverse inequality follows from Lemma 5.2. This completes the proof. □

It is thus seen that the formulas for $e_r(q,m)$ obtained in this section for $1 \leq r \leq m+1$ are of a different kind than those for $e_r(d,m)$ when $d < q$. The general pattern for $e_r(q,m)$ for $1 \leq r \leq \binom{m+q}{q}$ does not seem clear, even conjecturally. At any rate, it remains an interesting open problem to determine $e_r(d,m)$ for all the remaining values of r and m when $1 < d < q$ and also when $d = q$.

7 Acknowledgements

The authors would like to gratefully acknowledge the following foundations and institutions: Peter Beelen is supported by The Danish Council for Independent Research (Grant No. DFF–4002-00367). Mrinmoy Datta is supported by The Danish Council for Independent Research (Grant No. DFF–6108-00362). Sudhir Ghorpade is partially supported by IRCC Award grant 12IRAWD009 from IIT Bombay. Also, Peter Beelen would like to thank IIT Bombay where large parts of this work were carried out when he was there in January 2016 as a Visiting Professor. Sudhir Ghorpade would like to thank the Technical University of Denmark for a visit of 10 days in June-July 2016 during which this work was completed. We are also grateful to an anonymous referee for many useful comments and suggestions.

References

[1] M. Boguslavsky, On the number of solutions of polynomial systems, *Finite Fields Appl.* **3** (1997), 287–299.

[2] A. Couvreur, An upper bound on the number of rational points of arbitrary projective varieties over finite fields, *Proc. Amer. Math. Soc.*, **144** (2016), no. 9, 3671–3685.

[3] M. Datta and S. R. Ghorpade, On a conjecture of Tsfasman and an inequality of Serre for the number of points on hypersurfaces over finite fields, *Mosc. Math. J.* **15** (2015), no. 4, 715–725.

[4] M. Datta and S. R. Ghorpade, Number of solutions of systems of homogeneous polynomial equations over finite fields, *Proc. Amer. Math. Soc.* **145**, (2017), no. 2, 525–541.

[5] M. Datta and S. R. Ghorpade, Remarks on Tsfasman-Boguslavsky conjecture and higher weights of projective Reed-Muller codes, Arithmetic, Geometry, Cryptography and Coding Theory (Luminy, France, May 2015), Contemp. Math. **686**, Amer. Math. Soc., Providence, 2017, pp. 157–169.

[6] P. Heijnen and R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory* 44 (1998), no. 1, 181–196.

[7] M. Homma and S. J. Kim, An elementary bound for the number of points of a hypersurface over a finite field. *Finite Fields Appl.* **20** (2013), 76–83.

[8] G. Lachaud and R. Rolland, On the number of points of algebraic sets over finite fields, *J. Pure Appl. Algebra* **219** (2015), no. 11, 5117–5136.

[9] J.-P. Serre, Lettre à M. Tsfasman du 24 Juillet 1989, Journées Arithmétiques (Luminy, 1989). *Astérisque* No. 198-200 (1991), 351–353.

[10] A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (1991), 1567–1576.

[11] C. Zanella, Linear sections of the finite Veronese varieties and authentication systems defined using geometry, *Des. Codes Cryptogr.* **13** (1998), no. 2, 199–212.